EXHIBIT E

Tranche 1

SIM
Subscriber identity module
Subscriber identification module
Hack!
Swap!
Intercept!
Compromise!
Scam!
Verif!
Impersonat!
Imposter
Pretend!
Fake!
Faking
Pose!
Posing
Breach!
Defraud!
Authoriz!
Unauthoriz!

Tranche 2

Customer w/10 secur!
Customer w/10 fraud!
Customer w/10 access!
Customer w/10 id
Customer w/10 ident!
Customer w/10 priv!
Account w/10 secur!
Account w/10 fraud!
Account w/10 access!
Account w/10 id
Account w/10 ident!
Account w/10 priv!
Data w/10 secur!
Data w/10 fraud!
Data w/10 access!
Data w/10 id
Data w/10 ident!
Data w/10 priv!
Information w/10 secur!
Information w/10 fraud!
Information w/10 access!
Information w/10 id
Information w/10 ident!
Information w/10 priv!
Information w/10 personal

Tranche 3

Prime
Alorica
TPUSA

Commented [BM1]: These terms are too generic and are not reasonably tailored to identify relevant materials. For example, searching for "SIM" within a mobile telecommunications provider will return voluminous amounts of almost exclusively irrelevant materials without any connection to the issues in the case. This case involves unauthorized SIM changes, and we should be searching for documents addressing that, not isolated terms like "SIM," "swap," or "scam" – which would return voluminous amounts of irrelevant materials. The terms we proposed are designed to capture all references to an unauthorized SIM change.

We are willing to discuss the additional of certain of these terms if they are searched in connection with terms that would make it likely they appear in a document referencing an unauthorized SIM change, for example "imposter" w/10 "SIM." But bear in mind that our broad search for all instances of ("SIM SWAP!" or "SIM HIJACK!" or ("SIM CHANGE!" w/2 (UNAUTHORIZ! or FRAUD!))) should be sufficient to capture any such documents. If you believe the terms we've proposed are inadequate to capture relevant documents you intended these terms to return, we are happy to discuss that.

Commented [BM2]: These terms appear designed to capture any document referencing security of, or access to, any customer's account or information, without regard to the customer, the context, or any connection to SIM swapping or the incidents in this case. AT&T has already produced its confidential account security, fraud prevention, and customer authentication procedures and training materials, which would cover all relevant information relating to the policies, procedures, and training applicable to the security and privacy of plaintiff's account and information. We don't see how these terms are reasonably tailored to capture additional documents relevant to the case.

We are happy to discuss these further if you can elaborate on what additional relevant materials, beyond what we have already provided, you are seeking through these.

Teleperformance
Concentrix
Convergys

Tranche 4

CPNI
Customer Proprietary Network Information

Tranche 5

Consent w/10 decree
Consent w/10 order
Comply w/10 decree
Comply w/10 order
Compliance w/10 decree
Compliance w/10 order
Compliance w/10 report
Compliance w/10 office!
Compliance w/10 plan!
FCC
Federal Communications Commission
Information Security Program
Risk Assessment

Commented [BM3]: These terms, searched in isolation, are too generic and would return countless irrelevant documents about these entities. We can see potential relevance in documents referencing these entities in connection with a discussion of Mr. Williams (or his account) or unauthorized SIM swaps, but note that the search terms we've proposed are already designed to capture all such documents. Also, AT&T has already produced its security, customer authentication, fraud prevention and privacy policy and training materials applicable to these entities. We are happy to discuss this further if you can elaborate on what additional relevant materials about these entities that you are seeking.

Commented [BM4]: These have the same problem as Tranche 1 re: being too generic, especially when searched in isolation as you've proposed. A term as generic as "CPNI" -- particularly when searching the records of a telecommunications provider -- would return countless documents having no connection to the events in this case. While we can see potential relevance in searching for documents referencing "CPNI" in connection with Mr. Williams or any unauthorized SIM changes on his account, the terms we've proposed are already broad enough to capture such documents.

More importantly, we still have seen nothing to indicate that any of Mr. Williams' CPNI was disclosed by AT&T to any third party. AT&T's Interrogatory No. 8 asked Mr. Williams to specifically identity any of his CPNI that was improperly disclosed, and his response only states that he believes "AT&T improperly provided third-party hackers with [his] SIM Card" and thus, any CPNI that it contained. That is not what happened in this case, as reflected by the account notes AT&T produced, which indicate Mr. Williams' SIM card and any data on it never left his phone or his possession. Those records illustrate that only Mr. Williams' connection to the AT&T network was transferred to a phone and SIM card already in the hacker's possession. Without any indication that Mr. Williams' CPNI was improperly disclosed to the hackers, we do not see how searches for CPNI-related documents would return relevant materials in this case.

Commented [BM5]: These terms have the same issue as Tranche 4 in that they are not tailored to return documents relevant to the issues in this case. While we understand you are interested in documents related to the 2015 FCC Consent Decree, these type of overly broad terms (for example, "FFC," "Risk assessment") are far broader then necessary to capture such documents and would return voluminous amounts of materials with no connection to the Consent Decree or any issues in this case.

More importantly, we do not see any relevance in this case to the Consent Decree, which resulted from isolated incidents of rogue employees of call center vendors obtaining customers' SSNs to obtain phone unlock codes so subscribers could "jailbreak" their phones to switch to other providers (none of which happened in this case or has any connection to SIM swapping), and the FCC's investigation underlying the Consent Decree did not find any indication of SIM swapping or improper disclosure of CPNI in connection with those incidents. In all events, AT&T has already produced its policies, procedures and training materials related to account security and protection of customer information and CPNI. Without anything to suggest an improper disclosure of Mr. Williams' CPNI or personal information – which is what the Consent Decree was designed to address – we do not see how these terms, or documents concerning the Consent Decree, are relevant.

We are happy to discuss these further if you can elaborate on why you believe documents beyond what we've already produced and related to the Consent Decree are relevant to the incidents in this case.